Release Notes for Cisco Application Policy Infrastructure Controller Enterprise Module, Release 1.3.0.x

First Published: 2016-10-25

Release Notes for Application Policy Infrastructure Controller Enterprise Module, Release 1.3.0.x

This document describes the features, limitations, and bugs for this release.

Introduction

The Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM) is a network controller that helps you manage and configure your network.

The Cisco APIC-EM can support up to the following total number of devices, hosts, and access points:

- Network devices (routers, switches, wireless LAN controllers)—10,000
- Hosts—100,000
- Access Points—10,000

Note For specific Cisco APIC-EM requirements based upon the number of devices, hosts, and access points within your network, see Cisco APIC-EM Scale Requirements, on page 8.

What's New in Cisco APIC-EM, Release 1.3.0.x

Cisco is providing a software upgrade release that provides the following new features and functions:

- In this release, applications form separate deployment units. Supported applications can now be enabled to run on the controller or disabled on the controller. Each Cisco APIC-EM application consists of service bundles, meta data files, and scripts. For additional information about this new feature, see Cisco APIC-EM Application Separation, on page 3.

  The two supported applications for this release are IWAN and Network PnP.

- New Cisco APIC-EM **Dashboard** feature that is accessible from the controller's GUI home page.

  The **Dashboard** displays data through the use of individual widgets. Displayed data includes:

  - **Device Inventory—**Number of devices and status
  - **Discovery-Unreachable Devices—**Number of discovered and unreachable devices
  - **Hosts—**Number of total hosts, as well as number of wired and wireless hosts
  - **Branch Sites—**Number branch sites and status
  - **Path Trace—**Number of path traces and status
  - **EasyQoS Scopes—**Number of scopes with and without policies
  - **PnP Projects—**Status of PnP projects

- Updated **Discovery** features, including:
  - Ability to configure Global CLI and SNMP settings as part of a single discovery job. In previous versions, you could only configure these Global settings through the **Settings** page.
  - Ability to find discovery jobs that have discovered a specified IP address.
  - Ability to edit a discovery job.
  - Improved graphical user interface (GUI) for easier configuration.

- **Host Filters—**You can now filter hosts by MAC address, IP address, host name, host type, connected network device IP address, or connected interface name.
- New **Device Controllability** feature**—**You can now apply SNMP credentials to your network devices (network devices without any existing SNMP credentials or without any matching SNMP credentials) during a discovery by enabling this functionality using the controller's GUI.
- New **Groups** functionality**—**As an administrator (ROLE_ADMIN), you can now set permissions for users to access and manage groups of network devices through a new RBAC scopes feature. User profiles now consists of access to user-created network device groups with RBAC scope, in addition to a specified role (administrator, policy administrator, observer, or installer) .
- New **EasyQoS** functionality, including Service Provider (SP) profiles, policy preview, policy restore to original configuration, policy restore to Cisco Validated Design (CVD), and other new features and functionality.
- New **Path Trace** support for DMVPN topologies.
- New Cisco APIC-EM security features including:
  - PKI subordinate certificate support
  - Configurable certificate lifetimes for network devices
  - New default tunneling configuration (Internet Protocol Security or IPsec) for inter-host communications

- New and updated Cisco APIC-EM system requirements: 32 GB RAM support for basic controller functionality including Inventory, Discovery, Topology, Path Trace, EasyQoS, and Network PnP (available for a limited network scale). For additional information, see Cisco APIC-EM Scale Requirements, on page 8.

Note The IWAN application requires an appliance, server, or virtual machine with more than 32 GB RAM.

- Resolution of several CDETs that enhance your controller's performance and stability.

You should upgrade your controller to Cisco APIC-EM release 1.3.0.x with this software upgrade patch. Refer to Upgrading to Cisco APIC-EM, Release 1.3.0.x, on page 13, in these release notes for information about the upgrade procedure.

Cisco APIC-EM Application Separation

With this release, Cisco APIC-EM treats applications as separate deployment units (separate from the controller platform). You can now enable or disable supported applications on the controller using the GUI.

To enable an application using the controller's GUI, in the **Home** window click either **admin** or the **Settings** icon (gear) at the top right corner of the screen. Next, click the **App Management** link from the drop down menu. This opens the **Application Management** window in the GUI. View the applications in this window. Click the **Enabled** button in the **Application Management** window to enable an application.

Note Prior to enabling or disabling an application, click on the information icon ("i" symbol within a blue circle) for specific application information, including whether you can disable it.

If you are upgrading from an earlier Cisco APIC-EM release, then the Cisco IWAN and Network PnP applications are installed and enabled by default. If you are installing the Cisco APIC-EM for the first time as a fresh install, then the Cisco IWAN and Network PnP applications are also enabled by default.

When enabling or disabling the IWAN and Network PnP applications, note the following:

- When enabling these two applications, you must first enable the Network PnP application and then enable the IWAN application.
- When disabling these two applications, you must first disable the IWAN application and then disable the Network PnP application.

For additional information about the application separation functionality, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

Cisco APIC-EM System Requirements

Cisco offers a physical appliance that can be purchased from Cisco with the ISO image pre-installed and tested. The Cisco APIC-EM can also be installed and operate within a dedicated physical server (bare-metal) or a virtual machine within a VMware vSphere environment. The Cisco APIC-EM has been tested and qualified to run on the following Cisco UCS servers:

- Cisco UCS C220 M4S Server
- Cisco UCS C220 M3S Server
- Cisco UCS C22 M3S Server

In addition to the above servers, the Cisco APIC-EM may also run on any Cisco UCS servers that meet the minimum system requirements (see Cisco APIC-EM Physical Server Requirements, on page 4). We also support running the product in a virtual machine that meets the minimum system requirements on VMware vSphere (see Cisco APIC-EM VMware vSphere Requirements, on page 5).

Note The Ubuntu 14.04 LTS 64-bit operating system is included in the ISO image and a requirement for the successful installation and operation of the Cisco APIC-EM. Prior to installing the Cisco APIC-EM on your Cisco UCS server, click the following link and review the online matrix to confirm that your hardware supports Ubuntu 14.04 LTS:

http://www.ubuntu.com/certification/server/

Cisco APIC-EM Physical Server Requirements

The following table lists the minimum system requirements for a successful Cisco APIC-EM server (bare-metal hardware) installation. Review the minimum system requirements for a server installation.

Note For Cisco APIC-EM scale requirements based upon the number of devices, hosts, and access points within your network, see Cisco APIC-EM Scale Requirements, on page 8.

The minimum system requirements for each server in a multi-host deployment are the same as in a single host deployment, except that the multi-host deployment requires two or three servers. Two servers are required for software high availability. Three servers are required for both software and hardware high availability. With multiple servers (two or three servers), all of the servers must reside in the same subnet. For additional information about a multi-host deployment, see Supported Multi-Host Configurations, on page 9.

Caution You must dedicate the entire server for the Cisco APIC-EM. You cannot use the server for any other software programs, packages, or data. During the Cisco APIC-EM installation, any other software programs, packages, or data on the server will be deleted.

Table 1: Cisco APIC-EM Physical Server Requirements

Physical Server Options	Server image format	Bare Metal/ISO

Hardware	CPU (cores)	6 (minimum) **Note** 6 CPUs is the minimum number required for your server. For better performance, we recommend using 12 CPUs.
	CPU (speed)	2.4 GHz
	Memory	32 GB (minimum) **Note** For specific Cisco APIC-EM scale requirements, see Cisco APIC-EM Scale Requirements, on page 8.
	Disk Capacity	500 GB of available/usable storage after hardware RAID
	RAID Level	Hardware-based RAID at RAID Level 10
	Disk I/O Speed	200 MBps
	Network Adapter	1
Networking	Web Access	Required
	Browser	The following browsers are supported when viewing and working with the Cisco APIC-EM: • Google Chrome, version 50.0 or later • Mozilla Firefox, version 46.0 or later

Cisco APIC-EM VMware vSphere Requirements

You must configure at a minimum 32 GB RAM for the virtual machine that contains the Cisco APIC-EM when a single host is being deployed. The single host server that contains the virtual machine must have this much RAM physically available.

For a multi-host deployment (2 or 3 hosts), only 32 GB of RAM is required for each of the virtual machines that contains the Cisco APIC-EM. Two servers are required for software high availability. Three servers are required for both software and hardware high availability. With multiple servers (two or three servers), all of

the servers must reside in the same subnet. For additional information about a multi-host deployment, see Supported Multi-Host Configurations, on page 9.

Note For Cisco APIC-EM scale requirements based upon the number of devices, hosts, and access points within your network, see Cisco APIC-EM Scale Requirements, on page 8.

Note As with running an application on any virtualization technology, you might observe a degradation in performance when you run the Cisco APIC-EM in a virtual machine compared to running the Cisco APIC-EM directly on physical hardware.

Table 2: Cisco APIC-EM VMware vSphere Requirements

Virtual Machine Options	VMware ESXi Version	5.1/5.5/6.0
	Server Image Format	ISO
	Virtual CPU (vCPU)	6 (minimum) **Note** 6 vCPUs is the minimum number required for your virtual machine configuration. For better performance, we recommend using 12 vCPUs.
	Datastores	We recommend that you do not share a datastore with any defined virtual machines that are not part of the designated Cisco APIC-EM cluster. If the datastore is shared, then disk I/O access contention may occur and cause a significant reduction of disk bandwidth throughput and a significant increase of I/O latency to the cluster.

Hardware Specifications	CPU (speed)	2.4 GHz
	Memory	32 GB (minimum) **Note** For specific Cisco APIC-EM scale requirements, see Cisco APIC-EM Scale Requirements, on page 8.
	Disk Capacity	500 GB
	Disk I/O Speed	200 MBps
	Network Adapter	1
Networking	Web Access	Required
	Browser	The following browsers are supported when viewing and working with the Cisco APIC-EM: • Google Chrome, version 50.0 or later • Mozilla Firefox, version 46.0 or later
	Network Timing	To avoid conflicting time settings, we recommend that you disable the time synchronization between the guest VM running the Cisco APIC-EM and the ESXi host. Instead, configure the timing of the guest VM to a NTP server. **Important** Ensure that the time settings on the ESXi host are also synchronized to the NTP server. This is especially important when upgrading the Cisco APIC-EM. Failure to ensure synchronization will cause the upgrade to fail.

VMware Resource Pools

When installing the Cisco APIC-EM on a VMware virtual machine, then we also recommend that you configure resource pools with the following settings.

- Resource Pools—CPU Resources:
  - Shares—Normal
  - Reservation—Minimum 14400 MHz
  - Reservation Type—Expandable
  - Limit—Maximum limit
- Resource Pools—Memory Resources:
  - Shares—Normal
  - Reservation—32 GB or 64 GB minimum depending upon your hardware
  - Reservation Type—Expandable
  - Limit—Maximum limit

For examples on how to create and configure both resource pools and a virtual machine for the Cisco APIC-EM, see Appendix B, "Preparing Virtual Machines for Cisco APIC-EM" in the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

Cisco APIC-EM Scale Requirements

The following table lists the Cisco APIC-EM appliance scale requirements for deployment.

Table 3: Cisco APIC-EM Appliance Scale Requirements

Hardware Appliance	Cores	RAM	Hard Disk	RAID	Scale Limits
APIC-EM-APL-R-K9	10	64 GB	4 X SAS HDD of 900 GB each	RAID 10	• 10,000 Network Device • 10,000 Access Points • 100,000 Hosts
APIC-EM-APL-G-K9	20	128 GB	8 X SAS HDD of 900 GB each	RAID 10	• 10,000 Network Device • 10,000 Access Points • 100,000 Hosts

The following table lists the Cisco APIC-EM virtual machine scale requirements for deployment.

Table 4: Cisco APIC-EM Virtual Machine Scale Requirements

Virtual Appliance	Cores	RAM[1]	Hard Disk	RAID	Scale Limits
Cisco APIC-EM installed on a Virtual Machine (32 GB)	12	32 GB	200 GB	RAID 10 (configured on the hardware)	• 500 Network Devices • 500 Access Points • 5000 Hosts
Cisco APIC-EM installed on a Virtual Machine (32 GB)	8	32 GB	200 GB	RAID 10 (configured on the hardware)	• 200 Network Devices • 200 Access Points • 2000 Hosts
Cisco APIC-EM installed on a Virtual Machine (64 GB)	6	64 GB	500 GB	RAID 10 (configured on the hardware)	• 1000 Network Devices • 1000 Access Points • 10,000 Hosts

1 32 GB of RAM supports basic controller functionality, including Inventory, Discovery, Topology, Path Trace, EasyQoS and Network PnP.

Supported Multi-Host Configurations

The Cisco APIC-EM supports a single host, two host, or three host cluster configuration. With a single host configuration, 32 GB of RAM is required for that host. With a two or three host cluster configuration, 32 GB of RAM is required for each host in the cluster.

Note Cisco APIC-EM does not support a cluster with more than three hosts. For example, a multi-host cluster with five or seven hosts is not currently supported.

The three host cluster provides *both* software and hardware high availability. The single or two host cluster only provides software high availability and does not provide hardware high availability. For this reason, we strongly recommend that for a multi-host configuration three hosts be used.

A hardware failure occurs when the physical host malfunctions or fails. A software failure occurs when a service on a host fails. Software high availability involves the ability of the services on the hosts to be restarted and respun. For example, on a single host, if a service fails then that service is respun on that host. In a two host cluster, if a service fails on one host then that service is re-spun on the remaining host. In a three host cluster, if a service fails on one host, then that service is re-spun on one of the two remaining hosts..

When setting up a two host or three host cluster, you should never set up the hosts to span a LAN across slow links. This may impact the recovery time if a service fails on one of the hosts. Additionally, when configuring either a two host or three host cluster, all of the hosts in that cluster must reside in the same subnet.

Cisco APIC-EM Licensing

The following are the licensing requirements for Cisco APIC-EM and its applications (apps):

- Cisco APIC-EM controller software and its basic apps (for example, Network PnP, Inventory, Topology, and EasyQoS):
  - No fee-based license is required. The controller software and basic apps are offered at no cost to the user.
  - You can download the controller software (ISO Image) and run it on bare-metal Cisco UCS servers or run the ISO image on a virtual machine in a VMware ESXi environment. In both cases, you need to ensure the required CPU, memory, and storage resources are available.
- Solution apps (for example, IWAN and any similar Cisco-developed solution app):
  - A per-device license is required to run the solution apps.
  - The solution apps licenses can only be acquired by purchasing Cisco® Enterprise Management 3.x device licenses, which also include the Cisco Prime™ Infrastructure licenses. The process for acquiring Cisco Prime Infrastructure 3.x device licenses is explained in the Cisco Enterprise Management Ordering Guide:

    Cisco Enterprise Management 3.x, Prime Infrastructure 3. x APIC-EM Ordering and Licensing Guides

Note The same license-acquisition process will also provide you with the right-to-use (RTU) licenses for APIC-EM solution apps. RTU licenses do not involve license files.

Cisco APIC-EM Technical Support

The following Cisco APIC-EM technical support options are provided:

- Cisco APIC-EM hardware appliance:

  Hardware support is provided through the Cisco SMARTnet® Service.
- Cisco APIC-EM controller, basic apps, and services:

  Cisco® TAC support is offered at no additional cost, if you have SMARTnet on any Cisco networking device.

- Cisco APIC-EM solutions apps and services:

  TAC support is offered at no additional cost, if you have a SWSS (maintenance contract) on Cisco® Enterprise Management 3.x device licenses.

Supported Platforms and Software Requirements

For information about the network devices and software versions supported for this release, see Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module.

Securing the Cisco APIC-EM

The Cisco APIC-EM provides many security features for the controller itself, as well as the hosts and network devices that it monitors and manages. We strongly suggest that the following security recommendations be followed when deploying the controller.

Table 5: Cisco APIC-EM Security Recommendations

Security Recommendations	Reference
Deploy the controller behind a firewall that does not expose the controller's management ports (for example, ports 22 and14141) to an untrusted network, such as the Internet.	See the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*, Security chapter, "Cisco APIC-EM Port Reference" for information about the key controller ports.
Configure IPSec tunneling for communications between the hosts in a multi-host configuration.	See the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*, Security chapter, "Configuring IPSec Tunneling for Multi-Host Communications" for information about configuring IPSec tunneling.
Configure Cisco APIC-EM HTTPS services to use TLS 1.1 or TLS 1.2, instead of TLS 1.0 (current default). TLS 1.2 is strongly preferred. However, ensure that your devices – especially those that will be introduced into the network using the Cisco APIC-EM PnP application also support TLS 1.1 and/or TLS 1.2 before choosing on a TLS version above 1.0. Additionally, make sure that any NB API consumers including the browser used to access the controller's UI are capable of communicating with TLS 1.1 or TLS 1.2. All of the browser clients supported by Cisco APIC-EM already support TLS 1.1 and above.	See the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*, Security chapter, "Configuring the TLS Version Using the CLI" for information about configuring the TLS version.

Security Recommendations	Reference
Replace the self-signed server certificate from the controller with one signed by a well-known Certificate Authority.	For this security recommendation, do one of the following: • See the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*, Settings chapter, "Importing a Certificate" for information about importing and using a certificate for the controller. • See the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*, Settings chapter, "Importing a Trustpool bundle" for information about importing and using a trustpool for the controller.
Configure a proxy gateway between the controller and the network devices it monitors and manages.	See the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*, Settings chapter, "Importing a Proxy Gateway Certificate" for information about importing and using the proxy gateway's certificate for the controller.
When using the controller's discovery functionality, use SNMPv3 with authentication and privacy enabled for the network devices.	See the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*, Settings chapter, "Configuring SNMP" for information about configuring SNMPv3 for the controller.

Deploying the Cisco APIC-EM

The Cisco APIC-EM supports the following deployment types:

- As a dedicated Cisco APIC-EM physical appliance purchased from Cisco with the ISO image pre-installed.
- As a downloadable ISO image that you can burn to a dual-layer DVD or a bootable USB flash drive.
- As a downloadable ISO image that you can install into a virtual machine within a VMware vSphere environment.

Note The USB flash drive must be bootable. You can use a third-party utility to create a bootable USB flash drive using the ISO image. You cannot boot from the USB flash drive if you copy the ISO to the flash drive.

To deploy the Cisco APIC-EM, refer to Chapter 5, “Deploying the Cisco APIC-EM,” in the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*. For a list of network devices supported for this release, see *Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module, Release 1.3.0.x*.

Note Before you deploy the Cisco APIC-EM, make sure that the time on the controller's system clock is current or that you are using a Network Time Protocol (NTP) server that is keeping the correct time.

Upgrading to Cisco APIC-EM, Release 1.3.0.x

You can upgrade to this Cisco APIC-EM release using the **Update** functionality of the controller's GUI. This upgrade procedure requires that you upload and update the new release, as described below.

Before You Begin

Review the following list of pre-requisites and perform the recommended procedures before upgrading your Cisco APIC-EM:

- You must have administrator (ROLE_ADMIN) permissions and access to all devices (RBAC Scope set to ALL) to perform this procedure.

  For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

- You can only upgrade to the new Cisco APIC-EM release from the following earlier software and software patch releases:
  - 1.2.1.691
  - 1.2.1.686
  - 1.2.0.1594
  - 1.1.2.15

Note If your current Cisco APIC-EM release version is not one of the above releases, then first upgrade to one of these releases prior to upgrading to this release.

- If you have not already done so, review the system requirements for your Cisco APIC-EM upgrade (see Cisco APIC-EM System Requirements, on page 3). The system requirements may have changed for this release from a previous release and may require that you make changes to your deployment.
- If you have not already done so, review the security recommendations for the Cisco APIC-EM (see Securing the Cisco APIC-EM, on page 11).
- Create a backup of your Cisco APIC-EM database. For information about backing up and restoring the controller, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.
- Prior to beginning the software update process for the Cisco APIC-EM, we recommend that you configure the idle timeout value in the **Auth Timeout** GUI window for at least an hour. If a user is logged out due to an idle timeout during the software update process, then this process will fail and need to be re-initiated again. For information about the procedure used to configure an idle timeout value, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

- Allocate the appropriate time for the upgrade process, upgrading from earlier releases to this Cisco APIC-EM release may take up to an hour to complete.
- If the upgrade fails, see the "Recovering from Upgrade Failures" chapter in the *Cisco Application Policy Infrastructure Controller Enterprise Module Upgrade Guide* for assistance.

Step 1 Download the Cisco APIC-EM upgrade package for this release from the Cisco website at the Download Software link.

Step 2 Upload the upgrade package to the controller using the **Update** functionality of the GUI.
For additional information about this step, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

Step 3 Update the controller's software with the upgrade package using the **Update** functionality of the GUI.
For additional information about this step, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

Step 4 After updating the controller's software with the upgrade package in the previous step, proceed to clear your web browser's cache.

Step 5 Check the controller's software version number in the GUI **SYSTEM INFO** tab, located in the **Home** window. The **SYSTEM INFO** tab should display the new software version.

New and Updated Applications

EasyQoS

EasyQoS supports the following new features and functionality:

- **Service Provider (SP) Profiles—**Service provider profiles define the Differentiated Services Code Point (DSCP), priority, and bandwidth for traffic that is destined for a service provider. You can use any of the four predefined SP profiles, or you can create a customized SP profile for your unique requirements.
- **Policy Preview—**You can preview the command line interface (CLI) commands that EasyQoS will send to a device when you apply the policy.
- **Policy Restore to Original Configuration—**The first time that you apply an EasyQoS policy configuration to devices, EasyQoS stores the original device configurations on the Cisco APIC-EM controller so that you can restore the original configuration onto the devices later, if needed.
- **Policy Restore to Cisco Validated Design (CVD)—**The Cisco Validated Design (CVD) configuration is the default configuration for the applications in EasyQoS. If you create or make changes to a policy and then decide that you want to start over, you can restore the Cisco Validated Design (CVD) configuration.
- **Policy Abort—**If you realize that you have made a mistake in a policy configuration, you can cancel the policy configuration process.
- **Policy Version Comparison—**You can view the differences between a selected version and the current version of a policy.

Note Within the EasyQoS application, Dynamic QoS is a beta functionality for this release.

For information about the new features and functionality, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Device and Inventory

Discovery and Inventory support the following new features and functionality:

- Added support for VSS (on the Catalyst 4000 and 6000 platforms) in inventory as per current support in Prime Infrastructure.
- Allow existing discovery job to be edited in place without having a new job displayed.
- Allow user to search for a discovery job.
- Geo-tagging of locations in the Device Inventory page.

For information about the new features and functionality, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Path Trace

Path Trace supports the following new features and functionality:

- Flow Analysis: Support for DMVPN tunnels

For information about the new features and functionality, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Caveats

Open Caveats

The following table lists the open caveats for this release.

Caveat ID Number	Headline
CSCvb24887	Currently, any user can delete any path trace request outside the scope. **Workaround**: There is no workaround at this time.

Caveat ID Number	Headline
CSCvb59572	On a Cisco APIC-EM multi-host cluster, an interruption of network communications between the hosts in the cluster may cause a RabbitMQ network partition. When this happens, the individual hosts may show a high CPU utilization and the cluster may become inaccessible. To confirm that the RabbitMQ has a network partition, log into the root on each of the hosts in the cluster and run the following command: **sudo rabbitmqctl cluster_status** If the "partitions" field of the command output on any host is not an empty list, then a RabbitMQ network partition has occurred. The following sample output shows the partitions field value with RabbitMQ network partition: `Cluster status of node 'rabbit@grapevine-root-1' ... [{nodes,[{disc,['rabbit@grapevine-root-1', 'rabbit@grapevine-root-2', 'rabbit@grapevine-root-3']}]}, {running_nodes,['rabbit@grapevine-root-3', 'rabbit@grapevine-root-1']}, {cluster_name,<<"rabbit@grapevine-root-1">>}, {partitions,[{'rabbit@grapevine-root-1', ['rabbit@grapevine-root-2']}]}]` **Workaround**: Run the **reset_grapevine** command on any one of the hosts in the multi-host cluster. When running this command, do not delete any virtual disks, authentication timeout policies, imported certificates, or backups when presented with the options to delete.
CSCux96848	When Delete Dynamic policy is initiated (same time for both Video and Voice), sometimes VOICE ACE's get deleted and sometimes VIDEO gets deleted, but not both at the same time. Both Voice and Video ACE's should be removed when delete dynamic policy is initiated. **Workaround**: There is no workaround at this time.

Caveat ID Number	Headline
CSCuy37443	The QoS statistics output "queueBandwidthbps" shows NA when configured with several commands. On an ISR router, configure the policy-map with the **bandwidth** and **priority** commands. Start a flow analysis with QoS statistics collection request with the ISR router in the path. This happens when configured with following commands: • **bandwidth percent** • **priority percent** • **priority** (strict priority) **Workaround**: There is no workaround at this time.
CSCuy36583	EasyQoS does not support custom app creation on an ASR 1000 (versions earlier than 3.13), if the first 3 alphabet letters match. **Workaround**: There is no workaround at this time.
CSCuy41584	VRF filters in **Topology** and **Inventory** will not work for Nexus platforms. **Workaround**: There is no workaround at this time.
CSCuy52361	Traffic will be disrupted when applying an EasyQoS policy on a Cisco Catalyst 4500 series switch that is using port channels. **Workaround**: When configuring EasyQoS on a Cisco Catalyst 4500 series switch using port channels, we recommend that you apply the EasyQoS policy during a maintenance window or by changing the routing metrics (either EIGRP or OSPF) to remove traffic off of the member links during the application of the policy.

Caveat ID Number	Headline
CSCuz74785	Any Cisco APIC-EM users who have been authenticated/authorized by an external server and who are locked out of the controller for whatever reason, cannot be manually un-locked. **Note** There is no GUI to show that the user is actually locked out. **Workaround**: There are two workarounds available: • Wait 15 minutes for the timeout to end before logging into the controller again. • Disable user locking for the specific user from the **Internal Users** window. **Note** You must have administrator privileges (ROLE_ADMIN) to perform this action.
CSCva32308	After erasing the exiting virtual disk and reconfiguring the RAID, attempts to install the ISO with a USB fail due to a mount issue. This issue is due to the following Ubuntu bug: https://bugs.launchpad.net/ubuntu/+source/debian-installer/+bug/1347726. **Note** This issue does not occur when using the CIMC for installation. **Workaround**: Unmount the /media and mount /cdrom.
CSCva36094	In some cases, EasyQoS provisioning on the Cisco Catalyst 3750x device with brownfield configuration fails due to the device providing a faulty status of its TCAM utilization. **Workaround**: Reload the device.

Caveat ID Number	Headline
CSCva39044	When a Cisco 2500 Series Wireless Controller (WLC) is upgraded from version 7.4.100.0 or lower to any version that EasyQos supports, EasyQos can push a policy to the WLC, but it cannot attach the WLAN. In this scenario, EasyQos should not push the policy to the WLC. Instead, it should display a message on the EasyQos GUI similar to the following: "AVC is not supported with the current bootloader version (1.0.16). Please upgrade the bootloader to version 1.0.18 or Field Upgradable software version 1.8.0.0 or higher. See Cisco documentation for information about Field Upgradable software." This issue is specific to the Cisco 2500 Series Wireless Controller (WLC). **Workaround**: Upgrade the wireless controller bootloader to version 1.0.18 or higher, perform an inventory synchronization, and reapply the policy.
CSCva68171	The underlying routing protocol to the cloud needs to be identified in a DMVPN path trace. **Workaround**: There is no workaround at this time.
CSCvb42765	An admin with partial RBAC scope cannot delete the groups that the admin created. **Workaround**: There is no workaround at this time.
CSCvb75641	You can incorrectly configure a user with both the ROLE_INSTALLER role and any other role at the same time. This should not be permitted, since there is no controller GUI access for the installer role. **Workaround**: There is no workaround at this time.

Caveat ID Number	Headline
CSCvb58195	An application may be omitted from the ACL due to limited TCAM resources, while higher rank applications are included in the ACL. When editing advanced settings for such NBAR applications in EasyQoS Policies window (e.g. change to bi-directional or add consumer application), it will still be omitted from the ACL in case of limited TCAM resources. **Workaround**: Mark the edited application as "Favorite" in the EasyQoS Application Registry screen. This will cause the application to be highly ranked and included in the ACL.
CSCvb59952	When configuring queuing policy on the Cisco 800 Series Integrated Services Routers, the attachment to the L2 interfaces will fail with the following message: "Configuration failed!". **Workaround**: There is no workaround at this time. Queuing policy is not supported on the L2 interfaces on the Cisco 800 Series Integrated Services Routers which run Cisco IOS 15.6.3M0a. Consider downgrading the Cisco IOS version on the devices.
CSCvb70665	The Cisco Catalyst 4000 with Cisco IOS image version 3.8.x/3.9.x fails to go into a managed state (inventory collection). This occurs when the Cisco IOS image version is greater than or equal to 3.8.x. **Workaround**: Use a Cisco IOS-XE image version less than or equal to 3.7.x.
CSCvb49220	In the EasyQoS application page, the unassigned count includes all devices that a user has access to; although, only devices for which the user is an admin are actually displayed. **Workaround**: There is no workaround at this time.

Caveat ID Number	Headline
CSCvb42765	The scoped admin user cannot delete their own groups. The user can disassociate himself from these groups, but only an admin with a global scope can delete the groups. **Workaround**: There is no workaround at this time.
CSCvb80940	With the EasyQoS application, policy preview is not displaying ACLs for the applications having consumer apps, although the policies are being pushed to the devices without any other issues. **Workaround**: There is no workaround at this time.
CSCvb83108	With the EasyQoS application:. • While creating a custom app, if the lower port range begins with zero, then while editing the custom app, the port range vanishes. You then need to reenter the port range to save it again. For example, after saving and editing, you will see blanks in the port range. • While creating a custom app, if there is a port value with a range and comma, then the custom app shows the lower range port value as a single value. For this reason, we recommend that you do not use a range and comma in a single port range. For example, if you create a port range of 11-20, 70, after saving you will see 11,70. **Workaround**: There is no workaround at this time.

Caveat ID Number	Headline
CSCvb50882	After upgrading to Cisco APIC-EM version 1.3.x, you will still have your discovery credentials available from your previous installation. If you run a legacy job specific discovery, then you may receive an error message. **Workaround**: Perform one of the following: • Select and only run a global discovery. • Select and run a global discovery with the job specific discovery. • Create a completely new job discovery and run it.
CSCvb86166	After a new installation of Cisco APIC-EM, version 1.3.x, if you edit a discovery with job specific credentials then you may receive an error message. **Workaround**: Perform one of the following: • Select and only run a global discovery. • Select and run a global discovery with the job specific discovery. • Create a completely new job discovery and run it.
CSCvb85200	When creating a policy and pushing a CVD in EasyQoS, if you attempt to abort this action while in progress and also perform a reset then a failure will occur. **Workaround**: Reapply the policy at the scope level, (only on the failed device). The policy will be configured and you should see success.
CSCvb86166	Running a cloned discovery job after disabling the job specific CLI credentials causes an error message. **Workaround**: Create a new discovery job or add new job specific CLI credentials to the discovery.

Caveat ID Number	Headline
CSCvb89681	After a network connectivity outage on a multi-host cluster, the "is_alive" status turns to "false" for one or more hosts and the services are harvested on those hosts. To check the host status, run the command **grapevine host display** on each host and check for the value of the attribute "is_alive" in the command output. This situation may occur if the network connectivity outage disrupts the RabbitMQ service, where this service is then unable to recover on its own. To further confirm that the symptom is caused by this condition, run the command**grapectl status grapevine_dlx_service** on each host within the cluster. The status of the grapevine dlx service status should be other than "RUNNING" on one or more hosts. **Workaround**: Run the **reset_grapevine** command on one of the hosts. When running this command, do not delete any virtual disks, authentication timeout policies, imported certificates, backups, or apps when presented with the options to delete.

Resolved Caveats

The following table lists the resolved caveats for this release.

Note For a list of caveats resolved in an earlier software release, see the Cisco APIC-EM release notes for that specific release.

Caveat ID Number	Headline
CSCva64675	Performance Monitor configuration fails for Cisco Cloud Services Router 1000V devices.
CSCva30089	For EasyQoS, the NBAR attributes are not supported for static protocols. **Workaround**: The defect was resolved only on Cisco IOS XE3.16.4 (which should be released shortly) , or if you are running older Cisco IOS XE3.16 releases , then you need to upgrade your protocol pack to Protocol Pack 22 or later.

Caveat ID Number	Headline
CSCuy18848	When defining class-maps for LAN queuing policies, the EasyQos app uses the meaning format of DSCP values. The EasyQoS app also uses the decimal format of DSCP values when defining policy-maps. The policy-map and class-map definitions should follow the same DSCP naming convention with the EasyQoS application.
CSCuy90109	A custom app is added to a class-map without being created in EasyQoS.
CSCuz61632	The **Claimed and Ignored** page count, on the lower-right corner of the **Network Plug and Play** window, displays "x of 0", where " x" is the cache value from **Unclaimed** page. The correct value should be "1 of 1".
CSCuz62005	VLAN ACLs are not identified in an ACL trace.
CSCuz78783	When running the **reset_grapevine** command on the evaluation version of Cisco APIC-EM (16 GB of memory), the cluster does not clean up the database. There is no issue with running the command on a Cisco APIC-EM cluster with 64 GB of memory.

Using the Bug Search Tool

Use the Bug Search tool to search for a specific bug or to search for all bugs in this release.

Step 1 Go to http://tools.cisco.com/bugsearch.

Step 2 At the Log In screen, enter your registered Cisco.com username and password; then, click **Log In**. The Bug Search page opens.

Note If you do not have a Cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

Step 3 To search for a specific bug, enter the bug ID in the Search For field and press **Return**.

Step 4 To search for bugs in the current release:

a) In the Search For field, enter APIC-EM and press **Return**. (Leave the other fields empty.)

b) When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by modified date, status, severity, and so forth.

Note To export the results to a spreadsheet, click the **Export Results to Excel** link.

Limitations and Restrictions

Cisco APIC-EM limitations and restrictions are described in the following sections:

General Limitations

- Path Trace: Cisco Performance Routing or PfR is not supported with DMVPN tunnels for this release.
- The web GUI may take a few seconds to begin after the controller is started.
- When working with the Cisco APIC-EM in a network with several thousand supported devices, the Topology window may load slowly. Additionally, filtering within the other controller windows may also proceed slowly.
- Up to 2046 IP addresses are supported per discovery scan.

Note The IP address limit applies for one or more configured IP ranges in the controller's GUI.

- The Cisco APIC-EM does not support duplicate IP addresses across VRFs in this release.
- Inventory and Topology VRF filters are only supported for Cisco IOS devices. Cisco non-IOS devices such as the Nexus devices are not supported with VRF filters.
- In a deployment with multiple inventory service instances running, re-sharding (rebalancing the devices to a remaining inventory instance when one of the inventory instances fails) occurs if any single inventory service instance fails. During this time, any device controlled by the failed service inventory instance displays in an inventory-collection pending state for a longer time than usual. Eventually, an inventory sync should occur without any issue

- We recommend that after deleting a user from the controller's database, that you do not reuse that username when creating a new user for at least 6 hours. This waiting period is required to ensure that the deleted user's access rights and privileges are not inherited when reusing the username.
- Cisco APIC-EM uses a master-slave database management system for the multi-host cluster. If the master host fails for any reason, then you will experience a 10 to 11 minute time interval when the controller UI is unavailable. This is due to the other two hosts recovering from that failure and re-establishing communications. If one of the slave hosts fail, there is no impact to the controller UI.

Multi-Host Limitations

- In a multi-host cluster with three hosts, if a single host (host A) is removed from the cluster for any reason, and the second host (host B) fails, then the last host (host C) will also immediately fail. To work around this limitation, perform the following procedure:

  1. Log into the last active host (host C) and run the **config_wizard** command.
  2. In the configuration wizard display, choose **<Remove a faulted host from this APIC-EM cluster>**
  3. In the configuration wizard display, choose **<Revert to single-host cluster>**

     The Grapevine services underpinning the original multi-host cluster are then removed and restarted.
  4. Access the displayed IP address with a browser to view the Grapevine developer console and view the progress as each service restarts.
  5. After host C is up and running, then proceed to reconfigure the multi-host cluster.

  Note For information about configuring a multi-host cluster, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

- To enable external authentication with a AAA server in a multi-host environment, you must configure all individual Cisco APIC-EM host IP addresses and the Virtual IP address for the multi-host cluster on the AAA server. For additional information about external authentication with the Cisco APIC-EM, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

Application Separation Limitations

- For this specific controller release, application bundles are only provided as part of the ISO image.
- When enabling or disabling an application on the controller, user downtime may result. For this reason, we recommend that you only perform these procedures during a maintenance time period.
- Once enabled, an application cannot be subsequently revoked and returned to its previous version or disabled status.
- After successfully enabling an application, you must log into the host and run the **reset_grapevine** command.

Important After entering this command, you are then prompted to delete virtual disks, user accounts, certificates, backups, etc. Be sure to select **n**, to not delete any of these pre-existing configurations and files.

- You should not attempt to enable or disable an application on a host within a multi-host cluster, if any one of the hosts within the multi-host cluster is down. If you do attempt to enable or disable an application in this situation, then the attempt will fail and a message will be displayed that the operation cannot be performed until all the hosts are up and running.
- As part of the application upgrade process, the controller only deletes the existing application that it successfully upgraded from in the controller's **grape application display** command output. The controller does not delete the record of any failed application upgrade attempts (stale application entries) in the controller's **grape application display** command output.

  For example, assume the last successful application installation version is 5.10 and attempts have been made to upgrade to other application versions (5.13, 5.14, and 5,15) which all failed due to various reasons. Assume that a successful upgrade was made to version 5.16. The following information will appear in the **grape application display** command output:

```
$ grape application display

apic-core                enable_time              "Tue Aug 02, 2016 10:39:37 PM"
apic-core                enabled                  true
apic-core                enabled_by_default       true
apic-core                in_transition            false
apic-core                last_error_code          null
apic-core                last_result              "Successfully upgraded
application=apic-core from version=5.10.1 to version=5.16"
```

```
$ grape application status

APPLICATION              VERSION         ENABLED         ENABLE TIME
-------------------------------------------------------------------------------------
apic-core                5.13            No              None
apic-core                5.14            No              None
apic-core                5.15            No              None
apic-core                5.16            Yes             Tue Aug 02, 2016 10:39:37 PM
```

  You can remove the stale application entries by using the **grape application remove** command, but this is not required for controller application separation functionality.

  The stale application entries will only appear in the controller's CLI command output. The stale application entries do not appear in the controller's GUI.

Security Limitations

- With this release, the default option for intra-host communications is IPSec and not GRE. If you choose not to use the default option and to configure GRE using the configuration wizard, then privacy is not enabled for all of the communications that occur between the hosts. For this reason, we strongly recommend that any multi-host cluster that is not configured with IPSec tunneling be set up and located within a secure network environment.
- The Cisco APIC-EM should never be directly connected to the Internet. It should not be deployed outside of a NAT configured or protected datacenter environment. Additionally, when using the IWAN or PNP

solution applications in a manner that is open to the Internet, you must configure a white-listing proxy or firewall to only allow incoming connections from your branch IP pools.

- The Cisco APIC-EM platform management service (Grapevine) running on port 14141 does not presently support installing a valid CA issued external certificate. We recommend that access at port 14141 using HTTPS via a northbound API or the Grapevine developer console be secured using stringent measures such as a segmented subnet, as well as strict source address-based access policies in the port's access path.
- Ensure that any external access to the Cisco APIC-EM using SSH (through port 22) is strictly controlled. We recommend that stringent measures be used, such as a segmented subnet as well as strict source address-based access policies in the port's access path.
- Ensure that the strict physical security of the Cisco APIC-EM appliance or server is enforced. For Cisco APIC-EM deployed within a virtual machine, ensure that strong and audited access restrictions are in place for the hypervisor management console.
- The Cisco APIC-EM backups are not encrypted when they are downloaded from the controller. If you download the backups from the controller, ensure that they are stored in a secure storage server and/or encrypted for storage.
- The **Update** button in the controller's **Trustpool** GUI window will become active when an updated version of ios.p7b file is available and Internet access is present. The **Update** button will remain inactive if there is no Internet access.
- As with any network management application, it is a general best practice to ensure that the traffic sent from Cisco APIC-EM to the managed devices is controlled in such a way as to minimize any security risks. More secure protocols (such as SSHv2 and SNMPv3) should be used rather than less secure ones (TELNET, SNMPv2), and network management traffic should be controlled (for example via access control lists or other types of network segmentation) to ensure that the management traffic is restricted to devices and segments of the network where it is needed.
- If you are currently using the Device PKI certificate management functionality for the network devices (for example, when using the IWAN App) and want to take advantage of the new feature to convert the private (internal) device PKI CA in the Cisco APIC-EM from Root CA mode to a Subordinate CA (or Intermediate CA to an external CA), then you must re-provision any of the Cisco APIC-EM provisioned network devices so they obtain the new PKCS12 bundle issued from this newly subordinated CA. If you later decide to convert the Cisco APIC-EM device PKI CA back to Root CA from Subordinate CA (also referred to as SubCA), then you need to reset the controller in order to accomplish this. Additionally, any devices provisioned with certificates by the Cisco APIC-EM in SubCA mode, need to be reprovisioned. For information about the new Cisco APIC-EM PKI certificate management functionality, see the *Cisco APIC-EM Deployment Guide*.
- The Cisco APIC-EM controller does not provide a GUI or an API for replacing a subordinate CA certificate. Once SubCA mode is enabled using the controller, then the only way to replace the certificate of the Device PKI CA is to do a complete reset that brings the controller back to default root CA mode. You must then redo the conversion to subordinate CA mode using a new subordinate CA certificate. Before converting the controller back to the SubCA mode, you must also remove all device ID certificates and keys issued to network devices under the previous configuration of the Device PKI CA. The devices must be taken off line before converting the controller to SubCA mode with the new subordinate CA certificate, and then all devices will need to be reprovisioned by the PKI broker service using the new configuration of the Device PKI CA.
- Currently, there is no subordinate CA certificate rollover capability available for the Cisco APIC-EM device PKI. This capability is targeted for a near future release. For this reason, we strongly recommend

that the subordinate CA certificate lifetime be set to at least two years. This will prevent any disruption to the device PKI due to a CA certificate expiration.

- When using the northbound REST API and creating a POST /trust-point request, this request must provide a trustProfileName attribute that has sdn-network-infra-iwan as its value (default). In the current release, no other values are valid for this required attribute.
- Due to a Cisco IOS XE crypto PKI import limitation, devices cannot import a PKCS bundle (made up of a device certificate, device key and the subordinate CA certificate) exceeding 4KB size. This problem occurs when the Cisco APIC-EM device PKI CA is changed to SubCA mode with a subordinate CA certificate that has several and/or lengthy X509 attributes defined, thereby increasing the size of the device PKCS bundle beyond 4KB. To circumvent this issue, get the subordinate CA certificate issued with very minimal attributes. For example, do not include CDP distribution and OCSP settings.

  The following command output is provided as an example of content from a subordinate CA certificate that can impact the file size, as well as the fields within the certificate where content should be minimized:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            2e:00:00:00:0e:28:d7:1f:24:a1:1e:ef:70:00:00:00:00:00:0e
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=com, DC=apic-em, CN=apic-em-CA
        Validity
            Not Before: Oct 18 19:56:54 2016 GMT
            Not After : Oct 19 19:56:54 2016 GMT
        Subject: CN=sdn-network-infra-subca
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:cd:a7:65:a4:c4:64:e6:e0:6b:f2:39:c0:a2:3b:
                    <snip>
                    85:a3:44:d1:a2:b3:b1:f5:ff:28:e4:12:41:d3:5f:
                    bf:e9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                D2:DD:FA:E4:A5:6A:3C:81:29:51:B2:17:ED:82:CE:AA:AD:91:C5:1D
            X509v3 Authority Key Identifier:
                keyid:62:6F:C7:83:42:82:5F:54:51:2B:76:B2:B7:F5:06:2C:76:59:7F:F8

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            1.3.6.1.4.1.311.21.7:
                0-.%+.....7.....#...I......^...Q...._...S..d...
    Signature Algorithm: sha256WithRSAEncryption
         18:ce:5b:90:6b:1d:5b:b4:df:fa:d3:8e:80:51:6f:46:0d:19:
```

Software Update Limitations

- Updating from earlier Cisco APIC-EM releases to this latest release may take up to an hour to complete.
- When updating from Cisco APIC-EM release version 1.2.x to 1.3.x and after *uploading* the upgrade package and starting the *update* process, you may see an error message in the **Update History** field of the controller's GUI (**Update** window). This error message states: "File has not been completed yet - There are missing chunk(s)". This error message is caused by an accidental double trigger for the update procedure. One of the triggered update operations in this procedure causes this error, and the other triggered update operation proceeds with the update without any problems.

In order to ensure that the second operation has in fact proceeded, you should:

- Log into the controller with your Linux credentials and check the /var/log/grapevine_manager_activity.log for the procedure's progress.
- If the update procedure is not in progress, then check the **Update History** field once again in the controller's GUI to ensure that the second operation completed successfully without any other problem.

- When updating Cisco APIC-EM in a virtual machine within a VMware vSphere environment, you must ensure that the time settings on the ESXi host are also synchronized to the NTP server. Failure to ensure synchronization will cause the upgrade to fail.
- Prior to beginning the software update process for the Cisco APIC-EM, we recommend that you configure the idle timeout value in the **Auth Timeout** GUI window for at least an hour. If a user is logged out due to an idle timeout during the software update process, then this process will fail and need to be re-initiated again.

  In case a failure occurs on a multi-host cluster during any software updates (Linux files) and you have not increased the idle timeout using the GUI, then perform the following steps:

  1. Log into each host and enter the following command: $ **sudo cat /proc/net/xt_recent/ROGUE | awk '{print $1}**'

     Note This command will list all IP addresses that have been automatically blocked by the internal firewall because requests from these IP addresses have exceeded a predetermined threshold.

  2. If the command in Step 1 returns an IP address, then perform a reboot on the host where the above command has been entered (same host as the user is logged in).

     Note The hosts should be rebooted in a synchronous order and never two hosts rebooted at the same time.

  3. After the host or hosts reboot, upload the software update package file to the controller again using the GUI.

Back Up and Restore

Important For the IWAN solution application, you must review the *Software Configuration Guide for Cisco IWAN on APIC-EM* before attempting a back up and restore. There is important and detailed information about how these processes work for the IWAN application that includes what is backed up, what is not backed up, recommendations, limitations, and caveats.

- Before attempting a back up and restore with a host in a multi-host cluster, note the following:

  - You cannot take a back up from a single host (not in a multi-host cluster) and then restore it to a host in a multi-host cluster.
  - You cannot take a back up from a host in a multi-host cluster and restore it to a single host (not in a multi-host cluster).

- When a user restores the controller from a backup file using the Cisco APIC-EM GUI, the password of the user will be reset to what is in that backup file.
- You can only restore a backup from a controller that is the same version from which the backup was taken. In addition to the controller version being the same as the backup, the enabled applications and version on the controller also need to be the same as the one on which the backup was taken.
- If you have configured a multi-host cluster with two or three hosts and not all of the hosts are running when you initiate a restore operation, then the restore operation will fail. All of the hosts that comprise the cluster must be in the cluster and operational at the time of the restore.
- Prior to beginning the backup and restore process for the Cisco APIC-EM, we recommend that you log out and then log back into the controller. This will ensure that the default forced session timeout for the Cisco APIC-EM does not occur during this process.
- Prior to beginning the backup and restore process for the Cisco APIC-EM, we recommend that you configure the idle timeout value in the **Auth Timeout** GUI window for at least an hour. If a user is logged out due to an idle timeout during the restore file upload process, then the restore process will fail and need to be re-initiated again.

Deployment Limitations

- For a multi-host deployment, when joining a host to a cluster there is no merging of the data on the two hosts. The data that currently exists on the host that is joining the cluster is erased and replaced with the data that exists on the cluster that is being joined.
- For a multi-host deployment, when joining additional hosts to form a cluster be sure to join only a single host at a time. You should not join multiple hosts at the same time, as doing so will result in unexpected behavior.
- For a multi-host deployment, you should expect some service downtime when the adding or removing hosts to a cluster, since the services are then redistributed across the hosts. Be aware that during the service redistribution, there will be downtime.
- The controller GUI starts up and becomes accessible prior to all the Cisco APIC-EM services starting up and becoming active. For this reason, you need to wait a few minutes before logging into the controller GUI under the following circumstances:
  - Fresh ISO image installation
  - Resetting the controller using the reset_grapevine command
  - Power failure and the controller restarts
- If you are installing the Cisco APIC-EM ISO image on a physical server using local media, you can use either a DVD drive, a bootable USB device, or a mounted VirtualMedia via CIMC (Cisco Integrated Management Controller for a Cisco UCS server). If you use a mounted VirtualMedia via CIMC, the installation process may take up to an hour. If you use a DVD drive or a bootable USB device, the installation process may take approximately 15 minutes.

- If you burn the APIC-EM ISO to a bootable USB flash drive and then boot the server from the USB flash drive, a "Detect and mount CD-ROM" error might display during installation. This typically occurs when you perform the installation on a clean, nonpartitioned hard drive. The workaround for the above issue is to perform the following steps:

  1. Press **Alt+F2** to access the shell prompt.
  2. Enter the **mount** command to determine the device that is attached to the /media mount point. This should be your USB flash drive.
  3. Enter the **umount /media** command to unmount the USB flash drive.
  4. Enter the **mount /dev/***device_path* **/cdrom** command (where *device_path* is the device path of the USB flash drive) to mount the USB flash drive to the CD-ROM. For example:
     ```
     mount /dev/sda1 /cdrom
     ```
  5. Press **Alt+F1** to return to the installation error screen.
  6. Click "Yes" to retry mounting the CD-ROM.

- When the configuration wizard is run to deploy the Cisco APIC-EM and the **<save & exit>** option is selected at the end of the configuration process instead of the **proceed>>** option, then you should always run the **reset_grapevine** command to bring the Cisco APIC-EM to an operational state. Failure to run the **reset_grapevine** command at the end of the deployment process after choosing the **<save & exit>** option in the configuration wizard will cause certain services to fail. The services that will fail are services that are brought up in the new VMs that are created and that depend upon the PKI certificates and stores. Services that do not depend upon the PKI certificates and stores will function properly.
- When you deploy the Cisco APIC-EM using the configuration wizard, you must create passwords that meet specific requirements. These password requirements are enforced for the configuration wizard, but are not enforced when accessing the controller's GUI.

Discovery Limitations

- HTTP and HTTPS are not supported for device discovery for this release.
- There is a 255 character limit when entering a multi-range IP address for a Discovery job. The Discovery job will fail if you enter more than 255 characters for a multi-range IP address.

User Account Limitations

- We strongly recommend that when creating usernames for the Cisco APIC-EM , that you always use the lowercase. Do not create two usernames that are the same, but have a different case. For example, do not create the following usernames: USER123 and user123.
- This version of the Cisco APIC-EM has been tested for external authentication with Cisco ISE based AAA servers, but it may support integration with other types of AAA servers.
- An installer (ROLE_INSTALLER) uses the Cisco Plug and Play Mobile App to remotely access the Cisco APIC-EM controller and trigger device deployment and view device status. An installer cannot directly access the Cisco APIC-EM GUI. If an installer needs to change their password, the admin must delete the user then create a new user with the same username and a new password.

- Users who are working with the controller's IWAN and PnP applications to monitor and manage devices and hosts must have their **Groups** values set to **All**. The IWAN and PnP applications do not support **Custom** groups. You set both roles and groups when configuring internal users in the **Settings** | **Internal Users** GUI window.

EasyQoS Limitations

- Custom apps created using the EasyQoS GUI application require an IP address (mandatory field). Custom apps created using the API do not require an IP address (optional field). Custom apps created without an IP address using the API will fail when applied to a NBAR router. NBAR routers do not support applications without an IP address. To apply the policy on NBAR routers, please remove the custom app from the list.
- When configuring EasyQoS on a Cisco Catalyst 4500 series switch using port channels, we recommend that you apply the EasyQoS policy during a maintenance window or by changing the routing metrics (either EIGRP or OSPF) to remove traffic off of the member links during the application of the EasyQoS policy. Traffic will be disrupted when the EasyQoS policy is applied on the port channel interfaces.
- When removing a network device from a scope in EasyQoS, options that permit you to restore to the original policy or delete the policy are not triggered. Additionally, unlike the option in EasyQoS that permits you to reapply a policy, there are no options to restore an original policy or to delete a policy when a policy fails on the network devices.
- For the EasyQoS application, the maximum number of devices that can be configured for a scope is 2000.
- Cisco EasyQoS is not supported on the Cisco ASR 1000 series router running Cisco IOS XE 16.3.1.
- Within the EasyQoS application, Dynamic QoS is a beta functionality for this release.

Important For specific EasyQoS feature support and restrictions by platform and line card, see *Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module*.

Path Trace Limitations

- VLAN ACLs (VACLs) are not supported for this release. The Cisco APIC-EM is only supporting ACLs on VLAN.
- For a NPR (Non Periodic Refresh) path scenario, after an upgrade, the controller will not refresh the path. Additionally, the statistics collection will stop. To continue the statistics collections, you must initiate a new path request.
- A path trace from a host in a HSRP VLAN to a host in a non-HSRP VLAN that is connected to any of the HSRP routers is not supported.
- Applying a performance monitor configuration through Cisco APIC-EM fails if there is a different performance monitor policy configuration on the interface. You should remove the performance monitor configuration on the interface and re-submit the path trace request.
- Because the Cisco Wireless LAN controllers (WLCs) do not send SNMP mobility traps, note the following:

- For a path trace request, the Cisco APIC-EM controller will not have the right egress virtual interface highlighted on any foreign WLC.
- The path trace request will also not highlight any ACLs applied on the foreign WLC.

The workaround is to wait for inventory cycle to complete.

- For Path Trace, Performance Monitor statistics are not supported for the Cisco ASR 1000 Series Aggregation Services Routers (Cisco IOS XE 16.3.1 image).
- For Path Trace, Performance Monitor statistics are not supported for the Cisco Catalyst 3850 Switch (Cisco IOS XE 16.2.X and 16.3.1 images). This is because of a limitation on this version which is release noted by the product:
  - http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/16-2/release_notes/ol-16-2-3850.html
  - http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/16-3/release_notes/ol-16-3-3850.html
- Cisco Adaptive Security Appliance (ASA) support is at a basic service level for this release, including Discovery and Inventory. There is no support for Cisco ASA in Path Trace and Topology, since Cisco ASA does not support CDP and it is not currently possible to identify link and path through the Cisco ASA appliance.

Important For specific path trace restrictions and support by platform, see *Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module*.

ACL Trace Limitations

- VLAN ACLs (VACLs) are not supported for this release. The Cisco APIC-EM is only supporting ACLs on VLAN.
- Object groups are not supported in an ACL trace.

Important For specific Path Trace ACL support by platform, see *Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module*.

Service and Support

Troubleshooting

See the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*, for troubleshooting procedures.

Related Documentation

The following publications are available for the Cisco APIC-EM:

Cisco APIC-EM Documentation

For this type of information...	See this document...
• Learning about the latest features. • Learning about the controller system requirements. • Reviewing open and resolved caveats about the controller.	*Cisco Application Policy Infrastructure Controller Enterprise Module Release Notes*
• Learning about supported platforms. • Learning about required configurations on certain specific platforms. • Learning about application-specific limitations on certain specific platforms.	*Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module*.
• Installing and deploying the controller. • Configuring credentials for device discovery. • Importing a certificate or trustpool. • Using service logs. • Configuring authentication timeout and password policies. • Monitoring and managing Cisco APIC-EM services. • Backing up and restoring the controller.	*Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*
• Navigating the Cisco APIC-EM GUI. • Getting familiar with the Cisco APIC-EM features.	*Cisco Application Policy Infrastructure Controller Enterprise Module Quick Start Guide*

For this type of information...	See this document...
• Creating user accounts. • Discovering devices in your network and populating your inventory. • Displaying discovered devices in various topological views. • Configuring quality of service on the devices in your network. • Performing path traces. • Using the topology map. • Accessing the Cisco APIC-EM APIs.	*Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*
• Troubleshooting the controller. • Troubleshooting services. • Troubleshooting passwords. • Working with the developer console. • Contacting the Cisco Technical Assistance Center (TAC).	*Cisco Application Infrastructure Controller Enterprise Module Troubleshooting Guide*
• Tasks to perform before beginning an update. • Updating the controller to the latest version. • Tasks to perform after an update.	*Cisco Application Infrastructure Controller Enterprise Module Upgrade Guide*

Cisco IWAN Documentation

For this type of information...	See this document...
Configuring the Cisco IWAN network.	*Cisco IWAN on Cisco APIC-EM Configuration Guide*[2] *Software Configuration Guide for Cisco IWAN on APIC-EM*
Reviewing open and resolved caveats about the Cisco IWAN application.	*Release Notes for Cisco Intelligent Wide Area Network Application (Cisco IWAN App)*

2 This is an updated and renamed version of the previous document, *Software Configuration Guide for Cisco IWAN on APIC-EM*.

Cisco Network Plug and Play Documentation

For this type of information...	See this document...
• Reviewing open and resolved caveats about Cisco Network Plug and Play. • Viewing the list of supported Cisco devices for Cisco Network Plug and Play.	*Release Notes for Cisco Network Plug and Play*
• Configuring Cisco Network Plug and Play.	*Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM* *Cisco Open Plug-n-Play Agent Configuration Guide*
• Learning about the Cisco Network Plug and Play solution. • Understanding the main workflows used with the Cisco Network Plug and Play solution. • Deploying the Cisco Network Plug and Play solution. • Using proxies with the Cisco Network Plug and Play solution. • Configuring a DHCP server for APIC-EM controller auto-discovery. • Troubleshooting the Cisco Network Plug and Play solution.	*Solution Guide for Cisco Network Plug and Play*
Using the Cisco Plug and Play Mobile App	*Mobile Application User Guide for Cisco Network Plug and Play* (also accessible in the app through Help)

APIC-EM Developer Documentation

The Cisco APIC-EM developer website is located on the Cisco DevNet website.

For this type of information...	See this document...
API functions, parameters, and responses.	APIC-EM API Reference Guide
Tutorial introduction to controller GUI, DevNet sandboxes and APIC-EM NB REST API.	Getting Started with Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM)

For this type of information...	See this document...
Hands-on coding experience calling APIC-EM NB REST API from Python.	APIC-EM Learning Labs

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation at:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

Notices

Trademarks